



## **State of Alaska State Security Office**

### **State of Alaska Cyber Security & Critical Infrastructure Cyber Advisory**

**August 2, 2016**

*The following cyber advisory was issued by the State of Alaska and was intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.*

**ADVISORY NUMBER:**  
SA2016-112

**DATE(S) ISSUED:**  
08/02/2016

**SUBJECT:**  
Multiple Vulnerabilities in Google Android OS Could Allow for Remote Code Execution

**OVERVIEW:**  
Multiple vulnerabilities have been discovered in the Google Android operating system (OS), the most severe of which could allow for remote code execution. Android is an operating system developed by Google for mobile devices including, but not limited to smartphones, tablets, and watches. These vulnerabilities could be exploited through multiple methods such as email, web browsing, and MMS when processing media files. Successful exploitation of these vulnerabilities could result in remote code execution in the context of the application, an attacker gaining elevated privileges, information disclosure, or bypassing security restrictions.

**THREAT INTELLIGENCE:**  
There are currently no reports of these vulnerabilities being exploited in the wild.

**SYSTEM AFFECTED:**  
· Android OS builds prior to versions 6.1 and Security Patch Levels earlier than August 05, 2016

**RISK:**  
**Government:**

- Large and medium government entities: **High**
- Small government entities: **High**

**Businesses:**

- Large and medium business entities: **High**
- Small business entities: **High**

**Home users:** **High**

## **TECHNICAL SUMMARY:**

Google's Android OS is prone to multiple vulnerabilities, the most severe of which could allow for remote code execution. The vulnerabilities are as follows:

- Remote code execution vulnerability in Mediaserver with the use of a specially crafted file (CVE-2016-2504, CVE-2016-3820, CVE-2016-3821)
- Remote code execution vulnerability in libjhead with the use of a specially crafted file (CVE-2016-3822)
- Elevation of privilege vulnerability in Mediaserver could allow for the execution of arbitrary code (CVE-2016-3823, CVE-2016-3824, CVE-2016-3825, CVE-2016-3826)
- Denial of service vulnerability in Mediaserver with the use of a specially crafted file (CVE-2016-3827, CVE-2016-3828, CVE-2016-3829, CVE-2016-3830)
- Denial of service vulnerability in system clock with the use of a specially crafted file (CVE-2016-3831)
- Elevation of privilege vulnerability in framework APIs allows a local malicious application to bypass operating system protections (CVE-2016-3832 )
- Elevation of privilege vulnerability in Shell may enable a local malicious application to bypass device constraints (CVE-2016-3833)
- Information disclosure vulnerability in OpenSSL could allow a local malicious application to access data outside of its permission levels (CVE-2016-2842)
- Information disclosure vulnerability in camera APIs could allow a local malicious application to access data structures outside of its permission levels (CVE-2016-3834)
- Information disclosure vulnerability in Mediaserver could allow a local malicious application to access data outside of its permission levels (CVE-2016-3835)
- Information disclosure vulnerability in SurfaceFlinger may allow a local malicious application to access data outside of its permission levels (CVE-2016-3836 )
- Information disclosure vulnerability in Wi-Fi may allow a local malicious application to access data outside of its permission levels (CVE-2016-3837)
- Denial of service vulnerability in system UI could enable a local malicious application to prevent 911 calls from a locked screen (CVE-2016-3838)
- Denial of service vulnerability in Bluetooth could allow a local malicious application to prevent 911 calls from a Bluetooth device (CVE-2016-3839)
- Remote code execution vulnerability in Qualcomm Qualcomm Wi-Fi driver could enable a remote attacker to execute arbitrary code (CVE-2014-9902)
- Remote code execution vulnerability in Conscrypt could enable a remote attacker to execute arbitrary code (CVE-2016-3840)
- Elevation of privilege vulnerability in Qualcomm components in which the most severe may allow a local malicious application could execute arbitrary code (CVE-2014-9863, CVE-2014-9864, CVE-2014-9865, CVE-2014-9866, CVE-2014-9867, CVE-2014-9868, CVE-2014-9869, CVE-2014-9870, CVE-2014-9871, CVE-2014-9872, CVE-2014-9873, CVE-2014-9874, CVE-2014-9875, CVE-2014-9876, CVE-2014-9877, CVE-2014-9878, CVE-2014-9879, CVE-2014-9880, CVE-2014-9881, CVE-2014-9882, CVE-2014-9883, CVE-2014-9884, CVE-2014-9885, CVE-2014-9886, CVE-2014-9887, CVE-2014-9888, CVE-2014-9889, CVE-2014-9890, CVE-2014-9891, CVE-2015-8937, CVE-2015-8938, CVE-2015-8939, CVE-2015-8940, CVE-2015-8941, CVE-2015-8942, CVE-2015-8943)
- Elevation of privilege vulnerability in kernel networking component could allow a local malicious application could execute arbitrary code (CVE-2015-2686, CVE-2016-3841)
- Elevation of privilege vulnerability in Qualcomm GPU driver could allow a local malicious application could execute arbitrary code (CVE-2016-2504, CVE-2016-3842)
- Elevation of privilege vulnerability in Qualcomm performance component could allow a local malicious application could execute arbitrary code (CVE-2016-3843)

- Elevation of privilege vulnerability in kernel could allow a local malicious application could execute arbitrary code (CVE-2016-3857)
- Elevation of privilege vulnerability in kernel memory system could allow a local malicious application could execute arbitrary code (CVE-2015-1593, CVE-2016-3672)
- Elevation of privilege vulnerability in kernel sound component could allow a local malicious application could execute arbitrary code (CVE-2016-2544, CVE-2016-2546, CVE-2014-9904)
- Elevation of privilege vulnerability in kernel file system could allow a local malicious application could execute arbitrary code (CVE-2012-6701)
- Elevation of privilege vulnerability in Mediaserver could allow a local malicious application could execute arbitrary code (CVE-2016-3844)
- Elevation of privilege vulnerability in kernel video driver could allow a local malicious application could execute arbitrary code (CVE-2016-3845)
- Elevation of privilege vulnerability in Serial Peripheral Interface driver could allow a local malicious application could execute arbitrary code (CVE-2016-3846)
- Elevation of privilege vulnerability in NVIDIA media driver could allow a local malicious application could execute arbitrary code (CVE-2016-3847, CVE-2016-3848)
- Elevation of privilege vulnerability in ION driver could allow a local malicious application could execute arbitrary code (CVE-2016-3849)
- Elevation of privilege vulnerability in Qualcomm bootloader could allow a local malicious application could execute arbitrary code (CVE-2016-3850)
- Elevation of privilege vulnerability in kernel performance subsystem could allow a local malicious application could execute arbitrary code (CVE-2016-3843)
- Elevation of privilege vulnerability in LG Electronics bootloader could allow a local malicious application could execute arbitrary code (CVE-2016-3851)
- Information disclosure vulnerability in Qualcomm components may allow a local malicious application to access data outside of its permission levels (CVE-2014-9892, CVE-2014-9893 CVE-2014-9894, CVE-2014-9895 CVE-2014-9896, CVE-2014-9897, CVE-2014-9898, CVE-2014-9899 CVE-2014-9900, CVE-2015-8944)
- Information disclosure vulnerability in kernel scheduler may allow a local malicious application to access data outside of its permission levels (CVE-2014-9903)
- Information disclosure vulnerability in MediaTek Wi-Fi driver may allow a local malicious application to access data outside of its permission levels (CVE-2016-3852)
- Information disclosure vulnerability in USB driver may allow a local malicious application to access data outside of its permission levels (CVE-2016-4482)
- Denial of service vulnerability in Qualcomm components could cause a temporary remote denial of service (CVE-2014-9901)
- Elevation of privilege vulnerability in Google Play services may allow bypassing of Factory Reset Protection (CVE-2016-3853)
- Elevation of privilege vulnerability in Framework APIs could be used to gain elevated capabilities without explicit user permission (CVE-2016-2497)
- Information disclosure vulnerability in kernel networking component could enable a local malicious application to access data outside of its permission levels (CVE-2016-4578)
- Information disclosure vulnerability in kernel sound component could enable a local malicious application to access data outside of its permission levels (CVE-2016-4569, CVE-2016-4578)
- Multiple Vulnerabilities in Qualcomm components including the bootloader, camera driver, character driver, networking, sound driver, and video driver (CVE-2016-3854, CVE-2016-3855, CVE-2016-3856)

Successful exploitation of these vulnerabilities could result in remote code execution in the context of the application, an attacker gaining elevated privileges, information disclosure, or bypassing security restrictions.

## **RECOMMENDATIONS:**

We recommend the following actions be taken:

- Apply appropriate updates provided by Google Android or mobile carriers to vulnerable systems, immediately after appropriate testing
- Remind users to download apps only from trusted vendors in the Play Store
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources

## **REFERENCES:**

### **Google:**

<https://source.android.com/security/bulletin/2016-08-01.html>

### **CVE:**

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2012-6701>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2014-9892>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2014-9893>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2014-9894>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2014-9895>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2014-9896>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2014-9897>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2014-9898>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2014-9899>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2014-9900>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2014-9901>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2014-9902>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2014-9903>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2014-9904>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2014-9964>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2014-9965>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2014-9966>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2014-9967>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2014-9968>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2014-9969>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2014-9970>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2014-9971>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2014-9972>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2014-9973>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2014-9976>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2014-9977>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2014-9978>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2014-9979>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2014-9980>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2014-9981>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2014-9982>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2014-9983>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2014-9984>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2014-9985>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2014-9986>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2014-9987>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2014-9988>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2014-9989>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2014-9990>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2014-9991>



<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2016-4578>